Comments On " Orbits of automorphism groups of fields"

Pramod K. Sharma
e–mail: pksharma1944@yahoo.com
School Of Mathematics, Vigyan Bhawan, Khandwa Road,
INDORE–452 001, INDIA.

Abstract

Let R be a commutative $k-$algebra over a field k. Assume R is a Noetherian integral domain and $|R| = \infty$. The group of $k-$automorphisms of R,i.e., $Aut_k(R)$ acts in a natural way on $(R - k)$. We study the structure of R when orbit space $(R-k)/Aut_k(R)$ is finite, and note that most of the results proved in [1, §2] hold in this case as well. We also give an elementary proof of [1,Theorem 1.1] in case k is finitely generated over its prime subfield.

1 Introduction

Let K/k be a non-trivial field extension. Authors in [1, §2] conjecture that the orbit space $(K - k)/Aut_k(K)$ is finite if and only if either both K and k are finite or both are algebraically closed. From the results of the authors, it is clear that K is finite if and only if k is finite. Moreover, if K is algebraically closed then so is k. About the converse, several results are proved. We prove here that if R is an infinite Noetherian integral domain which is a $k-$ algebra over a field k such that $|(R - k)/Aut_k(R)| < \infty$, then most of the results, not particularly relevant to fields, in [1, §2] hold.

2 Main Results

Throughout, we shall assume that R is an infinite commutative $k-$algebra over a field k which is Noetherian integral domain such that $|(R-k)/Aut_k(R)| < \infty$.

Theorem 2.1. *The field k is infinite and integrally closed in R.*

Proof: If $|k| < \infty$, then as $|(R-k)/Aut_k(R)| < \infty$, $|R/Aut_k(R)| < \infty$. Therefore $|R/Aut(R)| < \infty$. Hence by [2,Corollary 16], R is a finite field. This contradicts the fact that R is infinite. Hence $|k| = \infty$. Now, let $\alpha \in (R-k)$ be integral over k. Then for each $a \in k$, $a\alpha$ is integral over k, moreover, $\{a\alpha | a \in k\}$ is an infinite subset of $(R-k)$. Note that if $\beta \in (R-k)$ is integral over k, then for any $\sigma \in Aut_k(R)$, $\sigma(\beta)$ is integral over k. Hence orbit of β, i.e., $O(\beta) = \{\sigma(\beta) | \sigma \in Aut_k(R)\}$ is a finite set. This implies $|(R-k)/Aut_k(R)| = \infty$, a contradiction to the assumption that $|(R-k)/Aut_k(R)| < \infty$. Hence k is finite and integrally closed in R.

Theorem 2.2. *If characteristic of k is $p > 0$, then $k^p = k$ and $R^p = R$.*

Proof: Since k is integrally closed in R, $(R-k)^p \subset (R-k)$. Therefore

$$(R-k) \supset (R-k)^p \supset \cdots \supset (R-k)^{p^m} \supset \cdots$$

is a chain of orbit closed subsets of $(R-k)$ under the action of $Aut_k(R)$. Since $|(R-k)/Aut_k(R)| < \infty$, there exists $n \geq 1$ such that

$$(R-k)^{p^n} = (R-k)^{p^{(n+1)}}.$$

Thus for every $\lambda \in (R-k)$, there exists $\mu \in (R-k)$ such that

$$\begin{aligned} & \lambda^{p^n} = \mu^{p^{n+1}} \\ \Longrightarrow \quad & (\lambda - \mu^p)^{p^n} = 0 \\ \Longrightarrow \quad & \lambda = \mu^p \\ \Longrightarrow \quad & (R-k) = (R-k)^p \subset R^p. \end{aligned}$$

Now, if $\lambda \in (R-k), a \in k$, then

$$\lambda, (\lambda - a) \in (R-k) = (R-k)^p \subset R^p.$$

Assume $\lambda = \alpha^p, \lambda - a = \beta^p$ for $\alpha, \beta \in R$. Then

$$\begin{aligned} & (\alpha - \beta)^p = \alpha^p - \beta^p = a \in R^p \\ \Longrightarrow \quad & k \subset R^p \\ \Longrightarrow \quad & R = R^p \text{ since } (R-k) = (R-k)^p. \end{aligned}$$

Finally, as $R = R^p$ and k is integrally closed, $k = k^p$.

Theorem 2.3. *If $x \in (R-k)$ and $c \in k$, then there exists $\sigma \in Aut_k(R)$ such that $\sigma(x) = x + c$.*

Proof: The proof is similar to the proof of [1,Lemma 2.6].

Theorem 2.4. *If R is integrally closed, then $(R-k)^l = (R-k)$ for all $l \geq 1$.*

Proof: It suffices to prove the statement assuming l is a prime. In view of Theorem 2.2, we can assume that l is other than the characteristic of k. As in Theorem 2.2,

$$(R-k) \supset (R-k)^l \supset \cdots \supset (R-k)^{l^m} \supset \cdots$$

is a chain of orbit closed subsets of $(R-k)$. As $|(R-k)/Aut_k(R)| < \infty$, there exists $n \geq 1$ such that

$$(R-k)^{l^m} = (R-k)^{l^{(m+1)}}$$

for all $m \geq n$. Thus for any $\lambda \in (R-k)$, there exists $\mu \in (R-k)$ such that

$$\begin{aligned} & \lambda^{l^m} = \mu^{l^{(m+1)}} \\ \Longrightarrow \quad & (\lambda\mu^{-l})^{l^m} = 1 \\ \Longrightarrow \quad & \lambda\mu^{-l} \in R \end{aligned}$$

since R is integrally closed. Further, as k is integrally closed in R, $\lambda\mu^{-l} \in (k^*)_{l^m}$, the subgroup of $(l^m)^{th}$ roots of unity in k. Therefore $\lambda \in (R-k)^l(k^*)_{l^m}$ for all $m \geq n$. Consequently, $(R-k) \subset (R-k)^l(k^*)_{l^m}$. Next, for any $m \geq n$

$$(R-k)^{l^m} = (R-k)^{l^{2m}}.$$

Hence, as above, we can conclude that for any $\lambda \in (R-k)$, $\lambda \in (R-k)^{l^m}(k^*)_{l^m}$. Thus $(R-k) \subset (R-k)^{l^m}(k^*)_{l^m}$. We, now, consider two cases.
Case 1. $(k^*)_{l^m} \subsetneqq (k^*)_{l^{(m+1)}}$.

In this case, for any $c \in (k^*)_{l^m}$, there exists $b \in (k^*)_{l^{(m+1)}}$ such that $c = b^l$. Hence, as $(R-k) \subset (R-k)^l(k^*)_{l^m}$,we have

$$(R-k) \subset (R-k)^l(k^*)^l = (R-k)^l \subset (R-k).$$

Conquently, $(R-k)^l = (R-k)$.
Case 2. $(k^*)_{l^m} = (k^*)_{l^{(m+1)}}$ for all $m \geq n$.
We have

$$(R-k) \subset (R-k)^l(k^*)_{l^m} \subset (R-k)k^* \subset (R-k).$$

Consequently, $(R-k) = (R-k)^l(k^*)_{l^m}$ for all $m \geq n$. Further, we have also proved that

$$\begin{array}{ll} & (R-k) \subset (R-k)^{l^m}(k^*)_{l^m} \subset (R-k)k^* \subset (R-k) \\ \Longrightarrow & (R-k) = (R-k)^{l^m}(k^*)_{l^m} \\ \Longrightarrow & (R-k)^l = (R-k)^{l^{(m+1)}}(k^*)_{l^{(m-1)}} \end{array}$$

If $m > n$, then $m-1 \geq n$. Hence

$$(R-k)^l = (R-k)^{l^m}(k^*)_{l^m} = (R-k).$$

Thus the result follows.

Remark 2.5. If U is the set of units in R, and $U \cap (R-k) \neq \phi$, then $R^l = R$ and $k^l = k$.

We shall first prove that $U = U^l$. Let $v \in U \cap (R-k) = U \cap (R-k)^l$. Then $v = \lambda^l$ for some $\lambda \in (R-k)$. Clearly $\lambda \in U$. Hence $v \in U^l$. Therefore

$$U \cap (R-k) \subset U^l \cdots (i).$$

Next

$$U = [U \cap (R-k)] \cup [U \cap k^*] = [U \cap (R-k)] \cup k^* \subset U^l \cup k^* \cdots (ii)$$

We claim $k^* \subset U^l$. Let $a \in k^*$ and $\lambda \in U \cap (R-k)$. Then $\lambda a \in U \cap (R-k)$. Thus, by (i), $\lambda^{-1}(\lambda a) = a \in U^l$. Consequently $k^* \subset U^l$. Hence, by(ii), $U = U^l$. Now, let $a \in k^*$. Then there exists $b \in U$ such that $b^l = a$. Since k is integrally closed, $b \in k^*$. Hence $k = k^l$. This gives

$$\begin{array}{rcl} R^l & = & (R-k)^l \cup k^l \\ & = & (R-k) \cup k \\ & = & R. \end{array}$$

Hence the assertion holds.

Theorem 2.6. *If R is integrally closed, then $k = R^{Aut_k(R)} = \{\lambda | \sigma(\lambda) = \lambda$ for all $\sigma \in Aut_k(R)\}$.*

Proof: Let $\lambda \in R^{Aut_k(R)}, \lambda \notin k$. By [2,Lemma 5], λ is a unit. Therefore $L = R^{Aut_k(R)}$ is a field containing k. By Theorem2.4 , for any $l \geq 1, (R-k)^l = (R-k)$. Thus, since $\lambda \notin k$, $X^l - \lambda$ has no roots in k. Moreover, by Theorem 2.3, for every $a \in k$ and any root μ of $X^l - \lambda, \mu + a$ is also a root of $X^l - \lambda$ since for any $\sigma \in Aut_k(R), \sigma(\mu)$ is also a root of $X^l - \lambda$. As $|k| = \infty$, this is not possible. Hence $k = R^{Aut_k(R)}$.

Remark 2.7. : (i) If characteristic of k is $p \geq 0$, then we can drop the condition that R is integrally closed. This can be seen by taking $l = p$.
(ii) Under the conditions of the Theorem, $|O(\lambda)| < \infty$ if and only if $\lambda \in k$. If $|O(\lambda)| < \infty$, let $O(\lambda) = \{\lambda_1, \cdots, \lambda_t\}$. Then $(X-\lambda_1)\cdots(X-\lambda_t) = p(X) \in k[X]$. Hence each λ_i is integral over k, and consequently $\lambda \in k$. The converse is clear.

Theorem 2.8. *If $\lambda \in (R-k)$, then $S_\lambda = \{a \in k^* | \sigma(\lambda) = a\lambda$ for some $\sigma \in Aut_k(R)\}$ is a subgroup of finite index in k^*.*

Proof: Let $a, b \in S_\lambda$. Then there exist $\sigma, \tau \in Aut_k(R)$ such that $\sigma(\lambda) = a\lambda, \tau(\lambda) = b\lambda$. Therefore $\sigma\tau(\lambda) = ab\lambda$ and $\sigma^{-1} = a^{-1}\lambda$. Hence $ab, a^{-1} \in S_\lambda$. Thus S_λ is a subgroup of k^*. Now, assume $[k^* : S_\lambda] = \infty$. Choose an infinite set $\{b_1, \cdots, b_n, \cdots\}$ in k^* such that $b_i S_\lambda \neq b_j S_\lambda$ for $i \neq j$. We claim $O(b_i\lambda) \neq O(b_j\lambda)$ for all $i \neq j$. If not, then there exist $i \neq j$ such that

$$\begin{array}{rrcl} & O(b_i\lambda) & = & O(b_j\lambda) \\ \Longrightarrow & \sigma(b_i\lambda) & = & \sigma(b_j\lambda) \text{ for some } \sigma \in Aut_k(R) \\ \Longrightarrow & \sigma(\lambda) & = & b_i^{-1}b_j\lambda \\ \Longrightarrow & b_i^{-1}b_j \in & S_\lambda & \\ \Longrightarrow & b_i S_\lambda & = & b_j S_\lambda. \end{array}$$

As $b_i S_\lambda \neq b_j S_\lambda$ for $i \neq j$, the claim follows. This contradicts the assumption that $|(R-k)/Aut_k(R)| < \infty$. Hence $[k^* : S_\lambda] < \infty$.

Remark 2.9. If k is algebraically closed then $S_\lambda = k^*$. Hence for any $c \in k^*$, there exists $\sigma \in Aut_k(R)$ such that $\sigma(\lambda) = c\lambda$.
Let $[k^* : S_\lambda] = m < \infty$. Then for any $a \in k^*$, as k is algebraically closed, $(k^*)^m = k^*$. Thus $S_\lambda = k^*$, and the assertion follows.
(ii) Assume that R is integrally closed and $(R-k) \cap U \neq \phi$ where U is the

group of units of R. Then also the assertion of the Theorem holds ,i.e., we need not assume k to be algebraically closed in this case. This follows since $k^* = (k^*)^m$ by Remark 2.5.

In the end, we record an elementary proof of [1,Theorem 1.1] in case k is finitely generated over its prime field.

Theorem 2.10. *Let k be a field with $|k/Aut(k)| < \infty$. If k is finitely generated over its prime field, then k is finite.*

Proof: It is noted in [1] that characteristic of k is $p > o$ and it is perfect, i.e., $k^p = k$. Let $\mathbb{F}_p$ be the prime subfield of k. As k is finitely generated over $\mathbb{F}_p$, k has finite transcendence degree over $\mathbb{F}_p$. Let S be a transcendental basis of $k|\mathbb{F}_p$. Then $k|\mathbb{F}_p(S)$ is finite algebraic. If $S = \phi$, then clearly k is finite. Further, if $S \neq \phi$, then as k is perfect $k \neq \mathbb{F}_p(S)$. Thus $k|\mathbb{F}_p(S)$ is finite algebraic. As k is perfect, Frobenius endomorphism of k (say)σ is an automorphism. Therefore, as $[k : \mathbb{F}_p(S)] < \infty$, $\sigma(\mathbb{F}_p(S)) = \mathbb{F}_p(S)$. This, however, is not true. Consequently $S = \phi$, and k is finite.

REFERENCES

1. Kiran S. Kedlaya and Bjorn Poonen : Orbits of automorphism groups of fields, Jr. of Algebra, 293(2005), 167-184.

2. Pramod K. Sharma : Orbits of automorphisms of integral domains, Illinois Jr. of Mathematics(To appear).